GUIDELINES FOR IMPLEMENTATION OF THE STATE OF WASHINGTON HOMELAND SECURITY ADVISORY SYSTEM

FOR
TRIBAL, COUNTY AND LOCAL GOVERNMENT

Developed By The
Washington Military Department

March 31, 2003

For questions or recommendations on improvement of this guide, contact Mr. Joe Huden at (253) 512-8108 or e-mail joe.huden@mil.wa.gov. PLEASE NOTE: Additional guides have been prepared for state agencies and offices of elected officials; business, critical infrastructure and key assets; and citizens, neighborhoods and families. You may access these guides on-line at: http://emd.wa.gov/.

A Message from the Director, Washington Military Department

Homeland security begins at home. Citizens and government at all levels - federal, state, local and tribal – have a shared responsibility for defending against, deterring, and, if necessary, responding to terrorist acts such as the horrific attacks of September 11, 2001. Each of us must do our part to assure we're secure in the new threat environment. The more thorough we are in our advance planning, the better the chances of surviving and minimizing the impact of a terrorist attack.

This guide outlines a logical system for determining what protective actions are appropriate for your jurisdiction. I encourage you to use it in conducting a risk assessment and developing preparedness plans for your jurisdiction that are tied to each level of the national Homeland Security Advisory System.

The protection of employees, the survival of critical infrastructure and the continuity of government operations are vital to our safety and security. Elected officials and other government leaders must therefore treat emergency preparedness, continuity of government and delivery of essential services as one of government's highest priorities.   In addition to the information in this Guide, assistance is available from the Washington Military Department Emergency Management Division (http://emd.wa.gov/) and your local emergency management office. Information for contacting subject matter experts is set forth in an appendix to the guide.

As community leaders, we have a special obligation to anticipate and plan for terrorist-based threats and large-scale emergencies. We can make our communities safer by following the steps in this guide, by responding appropriately to threat advisories from the Department of Homeland Security (http://www.ready.gov), and by reporting unusual or suspicious behavior to the FBI and local law enforcement offices. Together, we can assure Washington remains a safe and secure place to live, work and raise our families.

> TIMOTHY J. LOWENBERG
> Major General
> Director, Washington Military Department

This guide is available on-line at the following web sites) (http://emd.wa.gov/   ) or (http://www.washingtonguard.com).

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This guidebook is designed to assist tribal, county and local governments in initiating standardized actions as the result of changes in the United States and the State of Washington Homeland Security Threat Condition Advisory Systems. It provides a framework for developing security response and deployment plans as well as act as a checklist when changes in the advisory are issued.

These recommendations have been developed in a generic format, which allows the government entity to develop specific implementation procedures appropriate for the size and complexity of the jurisdiction. Each recommendation should be reviewed to determine if it is applicable and appropriate to you or your government entity. The document developed by the tribal, county or local government office should contain as much detail as necessary to attempt to provide adequate levels of preparedness and security for the jurisdiction. Tribal, county and local units of government are encouraged to develop additional action steps as appropriate.

The specific recommendations for the color-coded Homeland Security Advisory Threat Condition Levels start on page 17. They are cumulative recommendations and should be used in combination to create your own plan.

Appendix A is a sample warning/alerting notification list, which you might want to expand upon and keep available for an emergency.

Appendix B is a sample risk assessment checklist. The checklist was developed by and is reprinted herein with the permission of WMD Consulting Group LLC, 808 Clearmount Rd, York, PA 17403, 717-332-0188. Government entities may find all or part of the checklist useful in conducting vulnerability assessments. The state Military Department makes no representations as to the accuracy, reliability, or validity of the checklist contents.

Appendix C defines the various terms and acronyms used throughout this document.

Appendix D is a list of general personal tips for consideration if a terrorist attack is imminent or has occurred.

Appendix E is a listing of County Emergency Management contacts.

Appendix F is a listing of Municipal Emergency Management contacts.

Appendix G is a listing of Internet address links to helpful information.

WASHINGTON MILITARY DEPARTMENT
STATE EMERGENCY MANAGEMENT DIVISION
CONTACT INFORMATION

Main Administrative Numbers: 253-512-7000 or 800-562-6108	
EMD Mailing Address:	Washington Military Department Emergency Management Division Building 20, M/S: TA-20 Camp Murray, WA 98430-5122

PLEASE NOTE. This document is provided as guidance to assist state planners in developing detailed homeland security response and deployment plans. While the guidance contained in this document is not considered confidential in nature, the state agency or office should consider whether the document it develops should be considered an exempt document, not for public disclosure (pursuant to RCW 42.17.310(ww) or other applicable exemptions). If the agency or office determines the document should be exempt, it is suggested that the document be labeled with citations to the applicable exemptions.

ASSIGNMENT OF HOMELAND SECURITY THREAT CONDITIONS

The Homeland Security Advisory System

	Color Code	Description
	RED (SEVERE)	SEVERE RISK of a terrorist attack (a terrorism attack has occurred or intelligence information indicates an imminent attack is probable)
	ORANGE (HIGH)	HIGH RISK of a terrorist attack (potential for an attack is high or intelligence indicates terrorists are actively seeking targets)
	YELLOW (ELEVATED)	SIGNIFICANT RISK of a terrorist attack (possibility of an attack or intelligence indicates terrorist activity)
	BLUE (GUARDED)	GENERAL RISK of a terrorist attack (threats may not be credible or corroborated but warrant a heightened alert)
	GREEN (LOW)	LOW RISK of a terrorist attack (no threats)

Homeland Security Threat Condition Considerations

Homeland Security Presidential Directive (HSPD)-3 (http://www.fas.org/irp/offdocs/nspd/hspd-3.htm) establishing the Homeland Security Advisory System ("HSAS") and the FBI's National Threat Warning System ("NTWS") provide factors for the assignment of Homeland Security Threat Conditions. The NTWS provides vital information regarding terrorism for the U.S. counterterrorism and law enforcement communities. The guidelines governing the NTWS also provide specific policy regarding public notification procedures.

HSPD-3 and NTWS guidelines contain certain criteria that should be considered when assessing threat risks. A decision on which Homeland Security Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, more than quantitative calculation. Higher Homeland Security Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. However, despite best efforts, there can be no guarantee that, at any given Homeland Security Threat Condition, a terrorist attack will not occur. Nonetheless, one important factor in determining a threat risk is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:

- ➢ The credibility of the threat.
- ➢ The level of corroboration regarding the threat.
- ➢ The degree to which the threat is imminent.
- ➢ Threat specificity, to include a specific target.
- ➢ The gravity of the consequences if threat is delivered.
- ➢ The assessed vulnerability of the target.

Target Vulnerabilities and Consequences

Terrorist threats range from disruptive vandalism to catastrophic attacks affecting large centers of population and vital infrastructure. With a specific threat of a terrorist attack it is necessary to determine what consequences would be realized if an attack were to occur. Some of the questions to be considered are as follows:

- ➢ Is the target strategically significant as to pose a major disruption to vital services and/or a loss of life?
- ➢ How would Federal, State and local governments, along with private industry and the American public, react to the loss and/or disruption of a particular target?
- ➢ If the threat is imminent, how much time exists for countermeasures to be implemented?
- ➢ Can a target be made less attractive through enhanced security measures?
- ➢ Can the threat be intercepted and neutralized by law enforcement or other state or federal government resources?
- ➢ Can the effected parties be warned and countermeasures implemented prior to the attack, hopefully, averting a loss of life?

At every Homeland Security Threat Condition level, the same critical attention to threat assessment methodology will be applied. It is recommended that all HSAS education and awareness programs emphasize that despite the best decision to assign an appropriate Homeland Security Threat Condition; there can be no guarantee that a terrorist attack will be prevented.

Federal and State Actions to Changes in Alert

NOTE: Actions are cumulative starting at GREEN level.

ALERT LEVEL	FEDERAL ACTIONS	STATE ACTIONS
RED (SEVERE)	Response is primarily directed toward public safety and welfare and the preservation of human life, including: ◆ Assigning emergency response personnel and pre-positioning of specially trained teams ◆ Monitoring, redirecting or	◆ If the threat is specific to Washington State, activate the state EOC to Phase IV operations, staffed with applicable state/federal agency representatives. ◆ If the threat is not specific to

ORANGE (HIGH) (continued from previous color band)	◆ constraining transportation systems ◆ Closing public and governmental facilities ◆ Increasing or redirecting personnel to address critical emergency needs	Washington State, activate the state Emergency Operations Center (EOC) to Phase III operations. ◆ Following assessment of the situation, if the event threatens or actually impacts the State of Washington, the Governor issues a proclamation of a state of emergency. ◆ Activation of a Joint Information Center (JIC) to include representatives from affected areas and agencies.
ORANGE (HIGH)	◆ Crisis management response will focus on law enforcement actions taken in the interest of public safety and welfare, and is predominantly concerned with preventing and resolving the threat. ◆ Consequence management response will focus on contingency planning and pre-positioning of tailored resources, as required.	◆ If the threat is specific to Washington State, activate the state EOC to Phase III operations, staffed with applicable state/federal agency representatives. ◆ If the threat is not specific to Washington State, provide double State Emergency Operations Officer (SEOO) staffing of the Alert and Warning Center. ◆ Prepare to, and if necessary, activate a JIC near the threatened area. Coordinate the release of information with appropriate local, county, state, tribal and federal agencies.
YELLOW (ELEVATED)	◆ Increasing surveillance of critical areas. ◆ Coordinating emergency plans with related agencies. ◆ Assessing further refinement of protective measures within the context of the current threat information. ◆ Implementing, as appropriate, contingency plans and emergency response plans.	◆ If the threat is specific to Washington State, activate the state EOC to Phase II enhanced operations and staff with additional SEOO. ◆ If the threat is not specific to Washington State, activate state EOC to Phase I. ◆ Update staff and agency liaison contacts list. ◆ Provide Public Information Officer (PIO) coverage.
BLUE (GUARDED)	◆ Checking communications with designated emergency response or command locations. ◆ Reviewing and updating emergency response procedures. ◆ Providing the public with necessary information.	◆ All state agencies prepared to staff the EOC as required. ◆ Normal operations with 24-hour EOC and SEOO. ◆ Additional staff alerted to the increased threat level.
GREEN (LOW)	◆ Refining and exercising preplanned protective measures. ◆ Ensuring personnel receive	◆ Normal operations with 24-hour EOC and SEOO.

	training on the Homeland Security Advisory System, departmental, or agency-specific protective measures. ♦ Regularly assessing facilities with vulnerabilities and taking measures to reduce them.	

State Emergency Operations Center Phases

Phase I - Routine Operations

Incidents are handled by the duty officer in cooperation with other local, state and federal agencies. Other staff may be involved as advisors if needed for specific expertise. The Duty Officer responds to incidents following established Standard Operating Procedures (SOPs) as outlined in the Washington Military Department Emergency Management Division Duty Officer Standard Operating Procedures.

Phase II - Enhanced Operations (Alert Stage)

An incident is or could potentially grow beyond the capability of the Duty Officer to handle. In this instance the Duty Officer, along with selected staff, are tasked to support the incident from the state EOC. At this phase, one or more persons may be initially tasked to provide specific emergency functions.

During this phase, the Duty Officer will continue to monitor and process other requests for assistance, separate from the incident that has caused activation of the EOC.

As a general rule, transition from Phase I to Phase II will automatically occur when:

- A local jurisdiction has activated its EOC
- The Division has deployed staff to the field
- Intelligence data indicates the potential for an emergency that is or may grow beyond the capability of affected local jurisdictions

Actions to be taken at this time may include:

♦ Response agencies actively assess the situation, gather intelligence from the field, and prepare to respond to the state and/or the affected local jurisdiction.

♦ The state EOC and other agency emergency operations functions are staffed in preparation for full activation. Key state agencies may be

requested to send representatives to state EOC.

♦ Liaisons are dispatched to local EOCs, field incident command centers or emergency-operating facilities (EOFs) as they are activated and requested by the local jurisdictions.

♦ Notification of the event and the alert actions are made to various government agencies and jurisdictions.

♦ The Governor's Communication Director disseminates public information regarding the state's alert actions. Information is provided to the Governor's Communication Director by the Military Department public affairs staff.

♦ The Governor, members of the Crisis Management Team, and/or state response personnel assess the potential emergency. Actions may include fly-over, ground visits to affected areas, consultations via phone with elected officials (e.g. neighboring governors, county commissioners), and other public appearances.

If additional staff support is required, the EOC Supervisor will have the authority to escalate to Phase III EOC activation or implement any other level of staffing that the situation may require.

Phase III - Full Operation

An incident's size and complexity requires representation in the EOC by appropriate state and outside agencies and organizations to support expanded operations. The number of staff and the agencies represented will vary by incident. In this phase, the level of activity dictates that normal EMD staff functions cease and all personnel support the incident.

Possible actions to be taken at this time include:

♦ The state EOC and other emergency operations functions are fully activated, with representation from appropriate state agencies, along with necessary federal agencies, local government and volunteer organizations. Requests from local governments for state assistance are prioritized and fulfilled commensurate with available resources.

♦ If requested, liaisons are dispatched to the field as the local EOCs or incident command centers are activated.

♦ The Crisis Management Team continues to assess the emergency, oversee state emergency actions, and advise the Governor's Chief of

Staff. In most cases, the Disaster Manager in the EOC will coordinate the actions of the Crisis Management Team and the Governor's Office during an emergency.

♦ If a formal proclamation of a state of emergency is recommended, the Governor's Chief of Staff will be briefed and provided the draft proclamation.

♦ Formal actions the Governor may take include, but are not limited to a proclamation of a state of emergency, activation of the National Guard, requests for Presidential Declaration, etc.

♦ The Governor, Crisis Management Team, and/or emergency response personnel continue to oversee and assess the emergency response. Actions may include fly-over, ground visits, and briefings by state agencies, etc.

♦ Continued notifications to local governments, neighboring states, federal agencies and provinces are made, informing them of state emergency actions and coordinating responses.

♦ The Governor's Communication Director activates public information team to handle all public information activities (from the state EOC and other locations as necessary).

♦ The Governor's Office and Crisis Management Team provide stakeholder management and maintain contact with neighboring states, the White House, the Congressional Delegation and State Legislators.

Phase IV – Catastrophic Operations

A major catastrophic event has occurred that exceeds the capability of state and local government to provide timely and effective response to meet the needs of the situation. An event of this magnitude could cause numerous casualties, property loss, and disruption of normal life support systems and significantly impact the regional economic, physical, and social infrastructures. As a general rule, transition to this phase occurs when the EOC is conducting response operations.
Actions to be taken at this time may include:

◆ The state EOC and other incident command posts are fully activated with representation from appropriate state agencies, along with necessary federal agencies, local government and volunteer organizations. Requests from local governments for state and federal assistance are prioritized and fulfilled commensurate with available resources and proclamations.

◆ One or more selected state level Emergency Support Functions (ESFs) has been activated to respond to the situation.

◆ FEMA Region X is notified and a Regional Operations Center (ROC) activated to establish links with the state EOC until the Federal Emergency Response Team (ERT) is established in the field.

◆ A Governor's Proclamation of a state of emergency is in effect and pending approval of a Presidential Declaration to allow use of federal assets.

◆ The Crisis Management Team continues to assess the emergency, oversee state emergency actions, and advise the Governor's Chief of Staff.

◆ The Governor, Crisis Management Team, and/or emergency response personnel continue to oversee and assess the emergency response. Actions may include fly-over, ground visits, and briefings by state agencies, etc.

◆ Continued notifications to local governments, neighboring states, federal agencies and provinces are made, informing them of state emergency actions and coordinating responses.

◆ The Governor's Communication Director activates a public information team and continues to handle all public information activities (from the state EOC and other locations as necessary).

♦ The Governor's Office and Crisis Management Team provide stakeholder management and maintain contact with neighboring states, the White House, the Congressional Delegation and State Legislators.
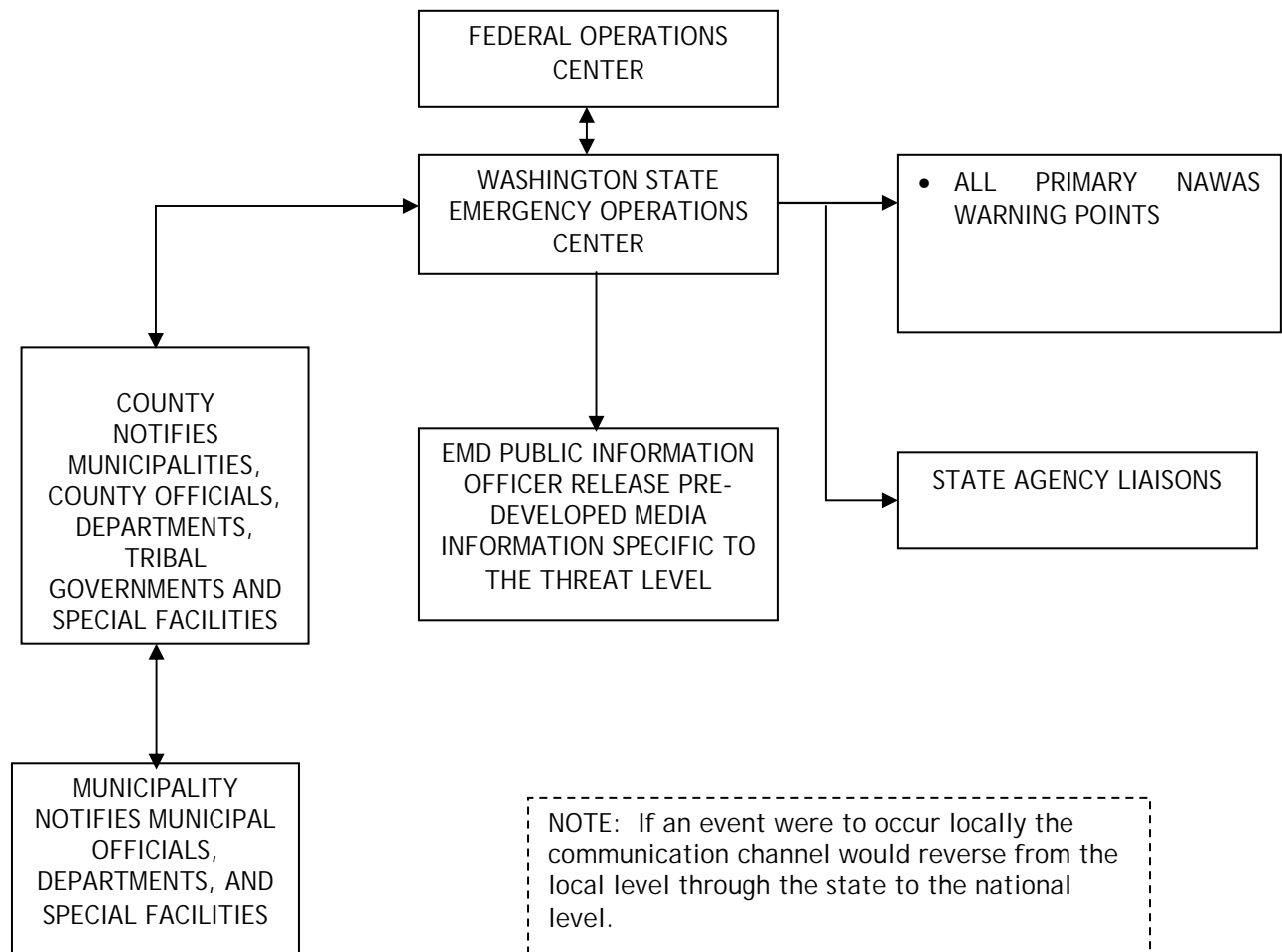
DISSEMINATION OF HOMELAND SECURITY THREAT CONDITION ADVISORIES WITHIN THE STATE OF WASHINGTON

Following notification of a change in the Homeland Security Threat Condition from the federal government, the Federal Operations Center will broadcast Homeland Security Threat Condition notifications over the National Warning System ("NAWAS") or other communications systems to all fifty states, including local warning points.

The State of Washington will disseminate Homeland Security Threat Condition advisory messages and other related strategic information within the state in the following manner (See Figure 1 on the next page):

1. The Washington Military Department, Emergency Management Division (EMD) will alert the following:
   a. Notify all Primary Warning Points using the National Warning System ("NAWAS").
   b. Disseminate the threat advisory via the statewide A Central Computerized Enforcement Service System ("ACCESS") message to all ACCESS terminals.
   c. Notify state government agency liaisons who will in turn be responsible for notifying their district and/or satellite offices.

2. Each county will be responsible for disseminating the Homeland Security Threat Condition advisory to appropriate county officials, departments and agencies, special facilities, tribal governments and designated municipal warning entry points (one per municipality).

3. Each municipality will be responsible for disseminating the Homeland Security Threat Condition advisory to its municipal officials, departments and to identified special facilities (schools, hospitals, industries, etc.).

4. Within thirty minutes after initial dissemination by EMD, the EMD Public Information Officer will authorize the release of pre-developed media information appropriate for the identified Homeland Security Threat Condition.

FIGURE 1 – HOMELAND SECURITY THREAT CONDITION DISTRIBUTION SYSTEM

```
                          ┌──────────────────────┐
                          │  FEDERAL OPERATIONS  │
                          │       CENTER         │
                          └──────────────────────┘
                                    ↕
                          ┌──────────────────────┐        ┌──────────────────────────┐
           ┌─────────────→│   WASHINGTON STATE   │───────→│ • ALL   PRIMARY   NAWAS  │
           │              │ EMERGENCY OPERATIONS │        │   WARNING POINTS         │
           │              │       CENTER         │        │                          │
           │              └──────────────────────┘        └──────────────────────────┘
           │                        │         │
           ↓                        ↓         │
  ┌──────────────────┐   ┌──────────────────────┐         ┌──────────────────────────┐
  │     COUNTY       │   │ EMD PUBLIC INFORMATION│  └─────→ │  STATE AGENCY LIAISONS   │
  │    NOTIFIES      │   │ OFFICER RELEASE PRE-  │         └──────────────────────────┘
  │  MUNICIPALITIES, │   │  DEVELOPED MEDIA      │
  │ COUNTY OFFICIALS,│   │ INFORMATION SPECIFIC TO│
  │   DEPARTMENTS,   │   │   THE THREAT LEVEL    │
  │     TRIBAL       │   └──────────────────────┘
  │ GOVERNMENTS AND  │
  │ SPECIAL FACILITIES│
  └──────────────────┘
           ↕
  ┌──────────────────┐
  │   MUNICIPALITY   │
  │ NOTIFIES MUNICIPAL│
  │    OFFICIALS,    │
  │ DEPARTMENTS, AND │
  │ SPECIAL FACILITIES│
  └──────────────────┘
```

NOTE: If an event were to occur locally the communication channel would reverse from the local level through the state to the national level.

RECOMMENDED TRIBAL, COUNTY AND LOCAL GOVERNMENT PROTECTIVE MEASURES

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	GREEN-LOW (LOW RISK of terrorist attack) Recommended Protective Measures:
G-1			Disseminate the GREEN advisory and share pertinent information related to the Homeland Security Threat Condition with tribal, county or municipal departments / agencies, emergency operations, fire districts, and government officials identified on the Warning / Alerting Notification List (Appendix A).
G-2			Identify critical facilities that may need protection. Budget for physical security measures.
G-3			Develop, review and/or update Emergency Response plans. Conduct training, seminars, workshops and exercises using the emergency response plans.
G-4			Develop or review, coordinate and exercise Mutual Aid agreements with other jurisdictions for use during emergencies.
G-5			Be alert to suspicious activities and / or individuals and report it to proper authorities or law enforcement agencies. Be suspicious of person(s) taking photographs of critical facilities, asking detailed questions about physical security or dressed inappropriately for weather conditions.
G-6			Routine operations without security stipulations are allowable. Possible security recommendations or considerations include: • Reviewing physical security precautions to prevent theft, unauthorized entry or destruction of property. • Providing access control and locking of high security areas. • Marking all security keys with "Do Not Duplicate."
G-7			Continue to include safety and common sense practices in daily routines. Conduct emergency preparedness training for citizens and employees. Provide emergency preparedness information to employees via paycheck inserts, tips, newsletters, articles and posters. Obtain copy of Terrorism: Preparing for the Unexpected brochure from your local Red Cross chapter. Obtain a copy of the United for a Stronger America: Citizens' Preparedness Guide from the National Crime Prevention Council (http://www.weprevent.org). Additional information on preparedness is available at Ready.Gov or by calling 1-800-BE-READY (1-800-237-3239).
G-8			Provide training on homeland security advisory system and physical security precautions.
G-9			Review staffing of emergency management and response functions. Recruit and train volunteers to augment full time staff, as appropriate. Contact Citizen Corps for potential volunteers (http://www.citizencorps.gov/).
G-10			Encourage employees to take Emergency Management, Red Cross first aid and Cardio-Pulmonary Resuscitation (CPR)/Automated External Defibrillator (AED) training.
G-11			Conduct routine inventories of emergency supplies and medical aid kits. Update and restock as required.
G-12			Encourage programs for employee immunizations and preventative health care.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

| Action Number | Checklist | | BLUE- GUARDED (GENERAL RISK of terrorist attack) Recommended Protective Measures: |
	Yes	No	
B-1			Disseminate the BLUE advisory and share pertinent information related to the Homeland Security Threat Condition with tribal, county or municipal departments / agencies, emergency operations, fire districts, and government officials identified on the Warning / Alerting Notification List (Appendix A).
B-2			Continue all measures listed in Homeland Security Threat Condition GREEN Advisory.
B-3			Review all applicable emergency plans (e.g. Emergency Operations Plan, Standard Operating Procedures (SOP) / Standard Operating Guides (SOG), personnel staffing schedules, internal security plans, Mutual Aid Agreements, etc., as applicable). Each department should be familiar with their assigned responsibilities according to the plan. Conduct tabletop and functional exercises as necessary, to increase familiarity with emergency plans and Mutual Aid agreements.
B-4			Implement security plans appropriate to the facility. Review communications plans and update the call-down procedures are current and accurate. Monitor and test communications and warning systems at periodic intervals. Possible security recommendations or considerations include: • Issuing employee picture ID badges. • Conducting background checks on employees, if authorized. • Installing surveillance cameras in vulnerable areas. • Providing a back-up power source for critical functions. • Installing an alarm system for critical buildings, doors or offices. • Moving vehicles and objects (trash containers, crates, etc.) away from buildings, particularly buildings of a sensitive nature. • Locking and regularly inspecting all buildings, rooms, and storage areas not in regular use.
B-5			Review and update public and private critical infrastructure target listings. Estimate the threat vulnerability of each critical facility and the countermeasures required to protect them.
B-6			Check all equipment for operational readiness, fill fuel tanks, check specialized response equipment (e.g. HAZMAT, SWAT, bomb squad, command post, generators, etc.), as appropriate.
B-7			Brief Public Information Officer (PIO) on appropriate response measures, protective actions, and self help options appropriate to the threat level. Activate the jurisdiction's Emergency Public Information System, as appropriate. Coordinate information releases with other government entities, if possible.
B-8			Assess mail handling procedures against intelligence in relation to the current Homeland Security Threat Condition. Advise personnel who handle mail, courier, and package delivery to remain vigilant and report any concerns or suspect items. Consider off-site mail / package processing and sorting facility to reduce the threat to government employees, if situation dictates.
B-9			Actively support the Neighborhood Watch, Community Emergency Response Team ("CERT"), Community Policing ("COP") and Amateur Radio Emergency Service ("ARES") (http://www.ares.org/) programs.
B-10			Evaluate information available on public websites that could compromise security.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist		YELLOW – ELEVATED (SIGNIFICANT RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
Y-1			Disseminate the YELLOW advisory and share pertinent information related to the Homeland Security Threat Condition with tribal, county or municipal departments / agencies, emergency operations, fire districts, and government officials identified on the Warning / Alerting Notification List (Appendix A).
Y-2			Continue all measures listed in the Homeland Security Threat Condition GREEN and BLUE Advisories.
Y-3			Implement critical infrastructure facility security plans as appropriate. Assess potential terrorist targets and develop additional plans, if necessary, to counteract an attack. Conduct additional vulnerability assessments of each critical facility and government building, as necessary. Assess the consequence of loss and assign a priority for their protection. Meet with appropriate representatives of critical infrastructure facilities to review contingency and evacuation plans and brief employees, as appropriate. Possible security recommendations or considerations include: • Increasing spot checks of specific high-risk targets / facilities. At the beginning and end of each work shift, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious or unattended packages. • Not leaving emergency response vehicles unattended. If it is necessary to leave the vehicle, lock it and check the vehicle and its chassis underside before opening the door and starting the engine. • Checking all deliveries to facilities.
Y-4			Check recall roster and recall processes for accuracy. Consider alternative work schedules of operational and staff personnel if the situation escalates. Include plans to maximize staffing and response capabilities with defined work / rest cycles.
Y-5			Consider plans and contingencies to assist public safety employees' family members regarding safeguard issues if the situation escalates and personnel are recalled leaving their family alone for extended periods of time.
Y-6			Identify any planned community events where a large attendance is anticipated. Consult with event organizers regarding contingency plans, security awareness, and site accessibility and control. Consider recommendations to cancel the event if warranted by the current situation.
Y-7			Increase the frequency of backups for critical information systems and review availability of technical support; e.g. systems programmers, technical personnel, redundancy of equipment, off-site storage of critical data, stockpile of critical spare parts, off-site data recovery, etc.
Y-8			Keep the public informed on current Homeland Security Threat Conditions and advisories.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist		ORANGE – HIGH (HIGH RISK of terrorist attack) Recommended Protective Measures:
	Yes	No	
O-1			Disseminate the ORANGE advisory and share pertinent information related to the Homeland Security Threat Condition with tribal, county or municipal departments / agencies, emergency operations, fire districts, and government officials identified on the Warning / Alerting Notification List (Appendix A).
O-2			Continue all measures listed in the Homeland Security Threat Condition GREEN, BLUE and YELLOW Advisories.
O-3			Activate the jurisdiction's Emergency Operations Center (EOC) for an initial situation briefing of EOC staff and government officials. Following the initial briefing maintain staffing, as warranted and appropriate.
O-4			Place all emergency management and specialized response teams on full alert status, as appropriate.
O-5			Review critical infrastructure and facility security plans and adjust accordingly. Possible security recommendations or considerations include: • Limiting access points to critical infrastructure facilities to the absolute minimum, and strictly enforcing entry control procedures. Locking all exterior doors except the main facility entrance(s). Identifying and protecting all designated vulnerable points. • Searching all suitcases, briefcases, packages, etc brought into a critical facility. • Checking all visitors' purpose, intent and identification. Checking that contractors have valid work orders outlining tasks to be performed within the secured facility. Requiring a visitor's sign-in log with information from their identification. Escorting visitors when they are in the facility, until they leave. Checking where the visitors were or worked to assure nothing is amiss or left behind. • Keeping critical response vehicles in a secure area or in an indoor facility. Keeping garage doors closed except for bona fide needs. • Enforcing parking of vehicles away from sensitive buildings. Erecting barriers and obstacles to control the flow of traffic, as appropriate. Visually inspecting the interior and undercarriage of vehicles entering parking lots and terraces. • Increasing defensive perimeters around key structures and events. Increasing security patrols around critical infrastructure facilities. Contacting allied government agencies within the jurisdiction and advise them of the need for increased security and awareness. • Coordinating closure of public roads and facilities that might make critical facilities more vulnerable to attack.
O-6			Determine if personal protective equipment (PPE) and specialized response equipment has been checked, issued, and readily available for deployment, if applicable
O-7			Suspend public tours of critical infrastructure facilities. Limit access to computer facilities.
O-8			Increase monitoring of computer and network intrusion detection systems and security monitoring systems. Determine if sufficient technical resources are available to respond to and mitigate a cyber attack.

NOTE: Protective Measures are cumulative and build from GREEN to RED. You may elect to use any or all of the recommended protective measures based on your particular situation. You may also elect to move a protective measure to a different alert level.

Action Number	Checklist Yes	Checklist No	RED - SEVERE (SEVERE RISK of terrorist attack) Recommended Protective Measures:
R-1			Disseminate the RED advisory and share pertinent information related to the Homeland Security Threat Condition with tribal, county or municipal departments / agencies, emergency operations, fire districts, and government officials identified on the Warning / Alerting Notification List (Appendix A).
R-2			Continue all measures listed in the Homeland Security Threat Condition GREEN, BLUE, YELLOW and ORANGE Advisories.
R-3			In the absence of a state proclamation of a state of emergency, consider a local proclamation/declaration to authorize activation of the local emergency management system.
R-4			Staff Emergency Operations Center (EOC) or Command Post on a 24-hour basis. Provide security for this facility.
R-5			Review critical infrastructure and facility security plans and adjust accordingly. Possible security recommendations or considerations include: • Making a positive identification of all vehicles located or operating within operational or mission support areas. • Making frequent checks of the exterior of critical facilities and begin spot checking of lower risk targets. Consider placing a security watch at all critical facilities 24-hours a day until the threat level has diminished. • Deliveries to critical facilities should not be accepted unless approved by supervisory staff. All deliveries should not be opened inside of the critical facility, and minimal personnel should be in the immediate area when the package is opened.
R-6			Consider releasing non-critical function personnel.
R-7			EOC has 24-hour access to the jurisdiction's Principal Executive Officer (e.g. County Executive, Mayor, City Manager) or their designated alternate.
R-8			Brief all EOC, government and first response personnel on critical facility evacuation routes and contingency communications plans. Provide direction regarding what equipment and supplies should be taken in the event of an evacuation.
R-9			Conduct welfare checks of government personnel and facilities throughout the day and night.
R-10			Activate, or place on high alert specialized response teams / personnel; e.g. HAZMAT, EMS, SWAT, Crisis Counseling, etc.
R-11			Be prepared to control access routes serving critical infrastructure facilities and evacuation routes.
R-12			Maintain communications with, and provide security for hospitals and critical medical facilities, if appropriate.
R-13			Stress the possibility of a secondary attack against first responders.
R-14			Assemble trained volunteers including: Community Emergency Response Teams ("CERT"), Community Policing ("COP") Teams, Amateur Radio Emergency Services ("ARES") teams.
R-15			Implement Mutual Aid agreements, as required.
R-16			Provide security for personnel dispatched to repair or restore damaged facilities and systems.

APPENDIX A

SAMPLE WARNING / ALERTING NOTIFICATION LIST
NOTE: This is just an example; include all necessary offices, facilities or people.

DATE		HOMELAND SECURITY THREAT CONDITION ADVISORY LEVEL	

NOTIFY	PHONE NUMBER	TIME NOTIFIED	PERSON CONTACTED	OPERATOR INITIALS
County Government				
County Executive				
County Elected Officials				
Sheriff				
Emergency Management				
Highway Department				
Local Government				
Mayor or City Manager				
Police Chief				
Fire Chief				
Emergency Management				
Critical Facilities/Key Assets				
Electric Utilities				
Water District				
Schools				
Hospitals				
Banks				

APPENDIX B

This risk assessment checklist was developed by and is reprinted herein with the permission of WMD Consulting Group LLC, 808 Clearmount Rd, York, PA 17403, 717-332-0188. Government entities may find all or part of the checklist useful in conducting vulnerability assessments. A checklist is also currently available electronically at *http://www.wmdconsulting.us/assess2.htm*. The state Military Department makes no representations as to the accuracy, reliability, or validity of the checklist contents.

Sample risk assessment checklist

TERRORISM VULNERABILITY SELF-ASSESSMENT

This vulnerability self-assessment is intended to help your organization determine if it is vulnerable to terrorism. When your self-assessment is shared with law enforcement, it will assist law enforcement with assessing the overall vulnerability of the community. It provides a vulnerability self-assessment worksheet that can be customized to your specific organization. The worksheet is intended to be a general guide. It may not include all issues that would be considered in your specific situation. Therefore, it is imperative that you consider the unique character of your organization: its functions, its general public image, and its overall public visibility. Consider both **who** may work in your organization and **what** your organization does. Assess the symbolic value of your organization to the public or within your own industry. This assessment does not replace any current any other assessment tools.

Most organizations or activities do not present a likely target for terrorism. Others' activities may make them a more likely terrorist target. Answering this self-assessment is a subjective process. It should be completed by a person knowledgeable of your organization. There are no firm guidelines on how to score a category. The score can best be determined by the person selected to complete the self-assessment, based on the uniqueness of your organization or facility. Since the questions are subjective, give your "best estimate" when scoring each question.

The Vulnerability Self-Assessment can also be used by law enforcement to assist in preventing criminal acts committed by terrorists. Preparation of a Threat Vulnerability Self-Assessment:

● is strongly recommended for local governments and, if completed, should be provided to the law enforcement agency that has primary first responder responsibility for each location of a local government office; and

● is strongly recommended for private businesses and should be submitted to the law enforcement agency which has primary first responder responsibility only if the Threat Assessment level is High Risk or if there are other significant factors warranting law enforcement's attention.

The Vulnerability Self-Assessment should be conducted at least annually and again if there is an increased threat of a terrorist event or whenever there is a significant change to your organization's facilities or activities.

Circle your evaluated score on each scale. Then total the scores and enter the total on the last page.

1. Potential Terrorist Intentions

Low Vulnerability	**Severe Vulnerability**

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Issues to be considered in selecting your score:

- Are you aware of any terrorist threat to your organization?

- Are you aware of a history of terrorist activity in your area or your specialty?

- Are you aware of the level of capability of any suspected terrorist which you believe poses a threat to your organization?

2. Specific Targeting

Low Vulnerability	**Severe Vulnerability**

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Issues to be considered in selecting your score:

- Have you obtained current information from law enforcement or other sources that your organization has been targeted by terrorists?

- What is the reliability of these information sources?

- What is your organization's public visibility?

- Does the nature of your organization's activity lead you to think it may be targeted?

- Are there activities that indicate possible terrorist preparations in your area or specialty?

3. Visibility of your Facility/Activity within the Community

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
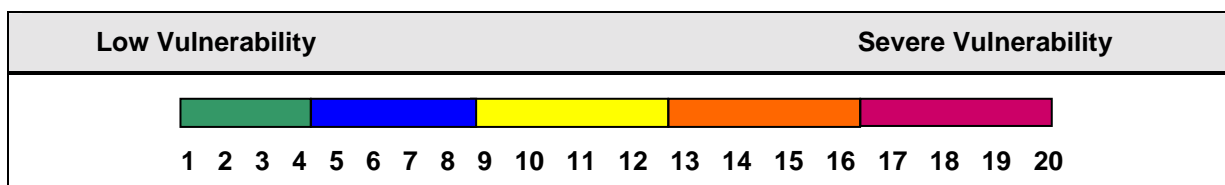
Issues to be considered in selecting your score

- Is your organization well known in the community?

- Do you regularly receive media attention?

- Is your organization nationally prominent in your field or industry?

- Is your location and the nature of your activity known generally to the public?

- Have you ever had an event or accident with potential health risks that attracted public attention to your facility?

- Does your facility work with animals that may make it a target of radical groups?

4. On-Site Hazards

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
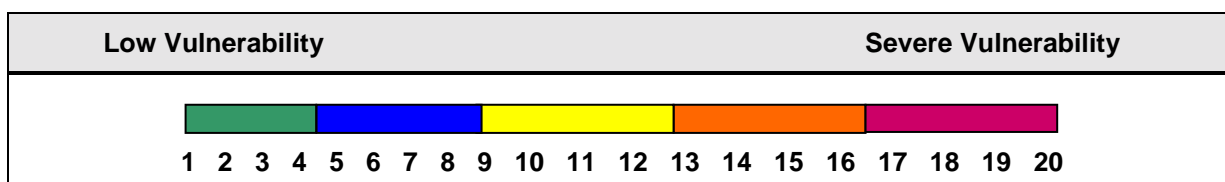
Issues to be considered in selecting your score:

- Are hazardous materials, explosives or other dangerous items on your site?

- Do you store or use biologic or chemical materials that have the potential to be used as a threat or weapon?

- Do you store or use radioactive material at your site?

- Do you have a system to control access to hazardous materials, explosives or any other dangerous materials at your site?

- Can any products stored or used on your site be used as, or in the manufacture of a mass casualty weapon?

- Can any products stored or used on your site cause extensive environmental damage?

5. Population of Site/Facility/Activity

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
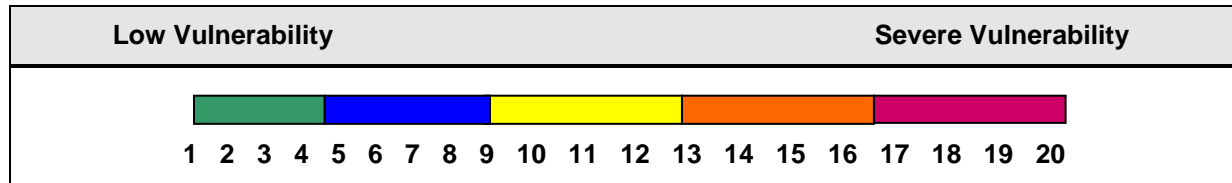
Issues to be considered in selecting your score:

- Do you have more than 250 people normally present at your site?
- Do you have more than 1,000 people normally present at your site?
- Do you have more than 5,000 people normally present at your site?
- Do you hold events at your site that attracts large crowds?
- Do you conduct public tours of your facilities?

6. Potential for Mass Casualties

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
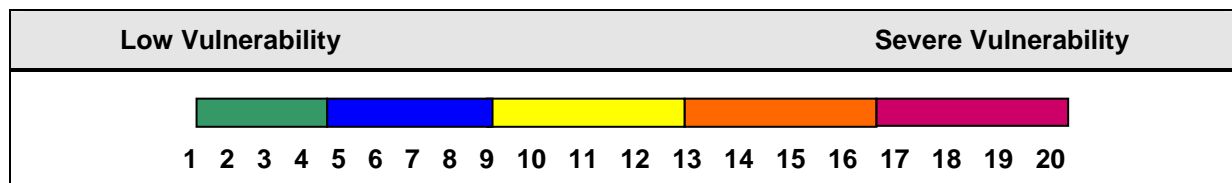
Issues to be considered in selecting your score:

- Do materials stored or used at your site have the potential to create mass casualties on-site?
- Do materials stored or used at your site have the potential to create mass casualties within 1 mile of your site?
- How many people live or work within one mile of your site: 500; 1,000; 2,000; 5,000; more than 5,000?

7. Security Environment & Overall Vulnerability to Attack

Low Vulnerability				**Severe Vulnerability**

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
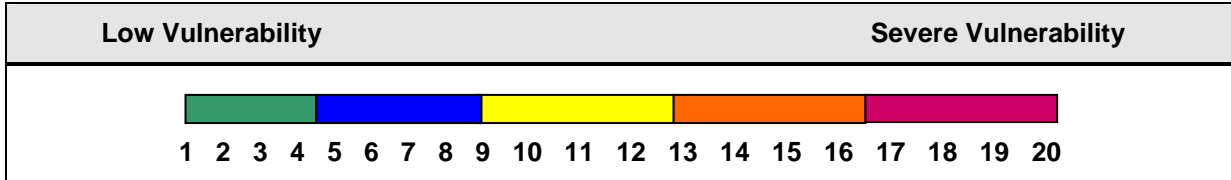
Issues to be considered in selecting your score:

- Does your organization have effective internal security procedures?

- What is the law enforcement presence in your area?

- What is the hardness, level of blast protection, etc. of your facilities?

- How accessible (security presence, access control, id badges, metal detection buffer zones, fences, etc.) is your facility?

- Are your assets and/or its potential recognized as a symbol?

- What level of public access is necessary for you to function?

- Can you control high-speed vehicle approaches to your facility?

- Do you have access control to your parking area?

- Do you conduct vehicle searches when entering facility grounds or parking areas?

- Do you employ detection/monitoring systems (video surveillance, intrusion detection systems, etc.)?

- Is your parking delivery area adjacent to or near your buildings?

- Is your delivery area supervised during hours of normal business?

- Is your delivery area access blocked during hours that your business is closed?

- Do you have an on-site food service facility for employees and visitors?

- Is access to the water supply for your facility protected?

- Is access to the ventilation system for your facility protected?

- Do you have a way to quickly shut down the water supply or ventilation system for your facility?

8. How Critical are your Products of Services?

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
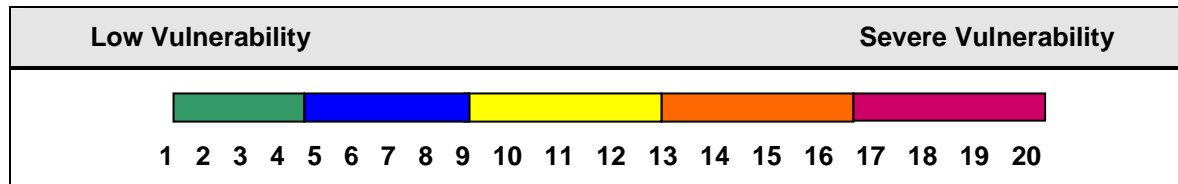
Issues to be considered in selecting your score:

- What is the importance of your organization to the community?

- What is the importance of your organization to your industry?

- Is your organization critical to the local population, economy or government?

- Is your organization critical to the continuity of basic services or utilities infrastructure in your area?

- Is your organization critical to state or national commerce?

- What would be the effects of a terrorist act against your organization?

- What would be the social, economic or psychological ramifications of a terrorist attack against your organization?

- What is the nature of your assets: hazardous materials, uniqueness, potential danger to others, etc?

- How long would it take to restore your critical services/functions?

9. High Risk Personnel

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
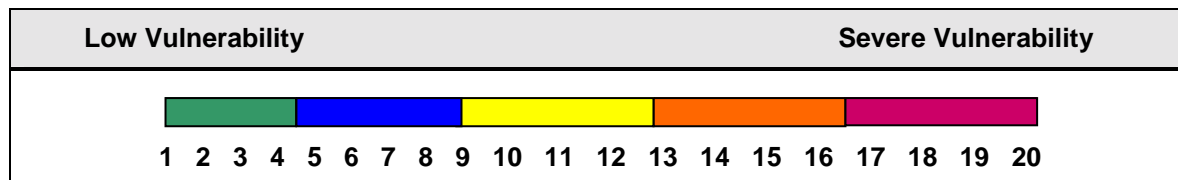
Issues to be considered in selecting your score:

- Do you have personnel that are critical to the continuing function of State or local government, basic services, utilities infrastructure, the community, the economy, or of inherent value to your business or agency?

- Do you have personnel that are critical for responding to a terrorist act?

- What would be the effect of a terrorist act against these high risk personnel?

10. Organization Communications

Low Vulnerability				Severe Vulnerability
1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17 18 19 20
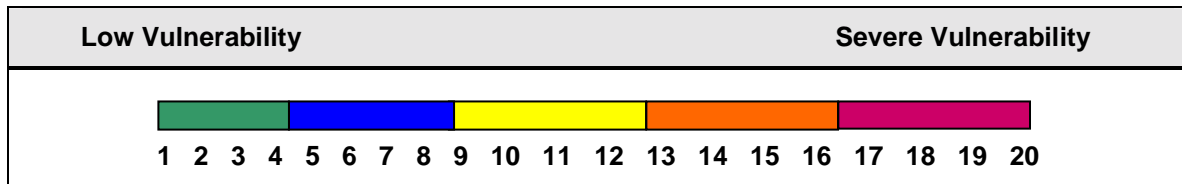
Issues to be considered in selecting your score:

- Do you have a Mass Notification System (public address system, intercoms, alarms)?

- Do you have a secure communications network that can be relied upon during a crisis?

- Do you have a crisis response team?

- Is your crisis response team trained?

- Do you conduct regular exercises?

- Do local/regional emergency responders participate in your exercises?

- Does your Crisis Response Team have its own portable communications system?

- Can your Crisis Response Team communicate directly with emergency responders?

- Do you have an emergency law enforcement notification system such as a hot line, panic button or something similar?

- Is your alarm system tied into the local law enforcement department or do you have an alarm service?

- Are your systems tested regularly?

11. Security and Response

Low Vulnerability				Severe Vulnerability
1 2 3 4	5 6 7 8 9	10 11 12	13 14 15 16	17 18 19 20
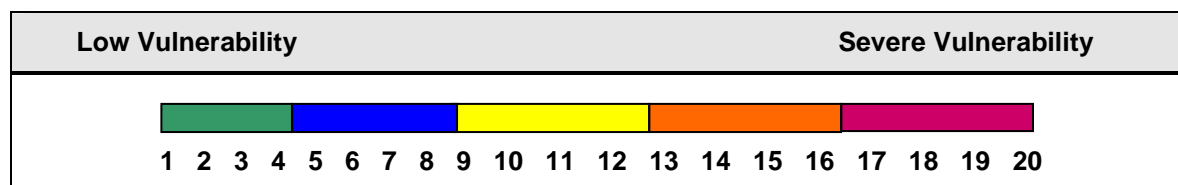
Issues to be considered in selecting your score:

- Are your security forces' staffing and training levels adequate?

- Do you have the capability to maintain a security presence in a high threat situation?

- Are additional security personnel available if requested?

- Are there affiliated agency/industry/organization support services available?

- Do you have trained disaster response teams within the organization?

- Do you have necessary specialty detection, monitoring, hazard assessment devices on hand and are they functional?

- Are local/regional law enforcement forces adequate and can they respond rapidly?

- Are local emergency responders familiar with your facility and its contents?

- Do you keep records on who visits your facility and where they go within the facility?

12. Policy/Procedures/Plans

Low Vulnerability				Severe Vulnerability
1 2 3 4	5 6 7 8 9	10 11 12	13 14 15 16	17 18 19 20
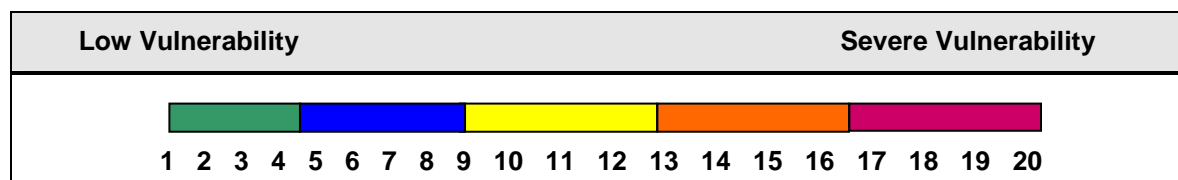
Issues to be considered in selecting your score:

- Do you have a current crisis response/disaster plan?

- Does your plan include the types of crises you are most likely to encounter (e.g., fire, explosion, chemical release)?

- Are your employees familiar with the plan?

- Have you conducted crisis response and disaster drills and were they effective?

- Have you identified the critical functions of your workplace and do you have a plan for continuation of operation during an emergency?

13. Security Equipment

Low Vulnerability				Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
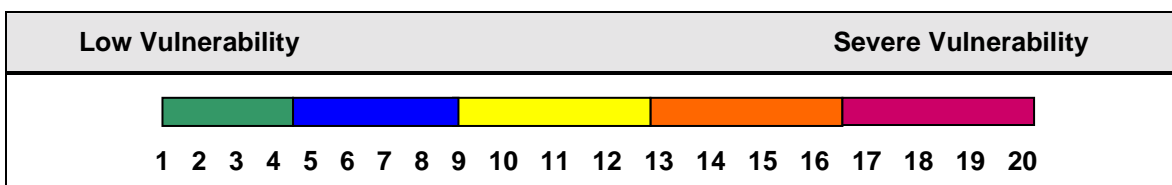
Issues to be considered in selecting your score:

- Do you have a security system and is it current technology?

- Do you have an intrusion monitoring motion detector or an alarm system?

- Do your systems have back-up if power is cut or fails?

- Do you have security equipment that would detect leaks or ruptures of potentially hazardous materials?

- Do you have personnel protective equipment for your emergency response team appropriate for the hazardous materials at your facility?

- Is such equipment in working order and has it been inspected recently?

14. Computer Security - Cyber-Crime & Cyber-Terrorism

Low Vulnerability				Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
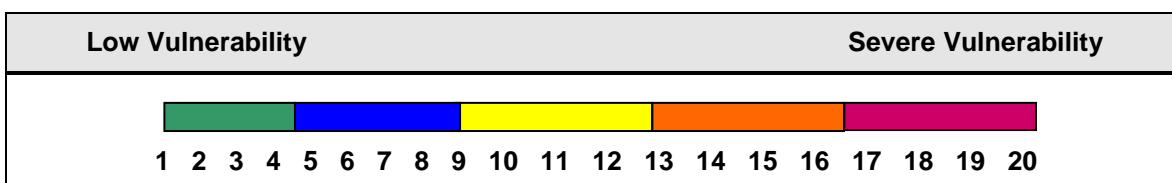
Issues to be considered in selecting your score:

- Is your site dependent on information technology such as computers and networks to accomplish its daily business activities?

- Is the information stored in your computer systems valuable?

- Do you have back-up power available for your computer systems?

- Do you make back-up copies of your data?

- Is your back-up data securely stored?

- Does your site have computers or networks connected to the Internet?

- Have you experienced problems with computer security incidents, such as computer viruses, worms, web-site defacements and/or denial of service attacks in the past?

- Do you have staff in place who are adequately trained and are available to monitor security warnings and take protective measures, such as loading system patches?

- Do you have technology security tools in place such as firewalls, intrusion detection systems or anti-virus software to protect your computer systems?

- Do you have a computer security policy, plan and procedure that includes a computer security incident response team?

15. Suspicious Mail And/Or Packages

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
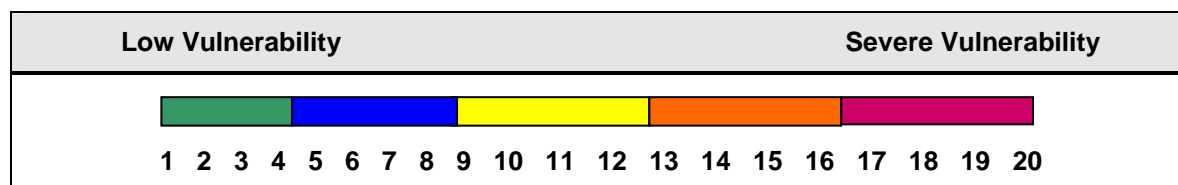
Issues to be considered in selecting your score:

- Is the mail for your facility opened in a secured area or an area isolated from the majority of personnel?
- Have the personnel who open mail received training on the recognition of suspicious mail and/or packages?
- Do you have specific procedures on how to handle suspicious mail and/or packages, including possible facility evacuation?
- Do you have a secure and contained location where any unusual or suspect deliveries or mail can be stored until proper authorities can evaluate the suspect items?

16. Telephone, Bomb And Other Threats

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
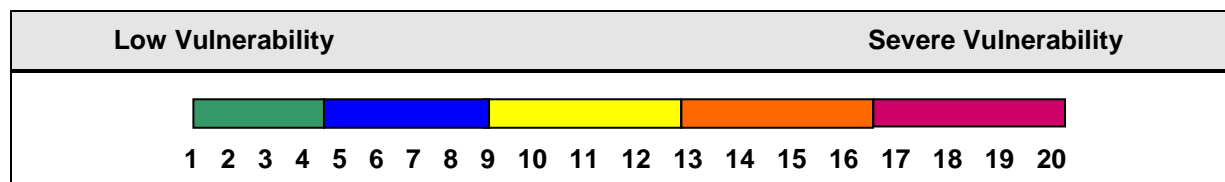
Issues to be considered in selecting your score:

- Has your staff received training on how to handle bomb and other threat calls?
- Does your staff have a checklist of questions to ask the caller in case of a bomb or other threatening call?
- Does your facility have a plan on how to handle bomb and other threatening calls?
- Does your bomb threat plan include a system whereby your personnel would search your facility to identify suspicious objects to point out to emergency response personnel?
- Does your plan include a decision making process on whether to evacuate the facility?
- Are personnel familiar with the plan? Have evacuation drills been conducted?
- Is your plan coordinated with local law enforcement and the local phone company?

17. Employee Health & the Potential for Bio-Terrorism

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
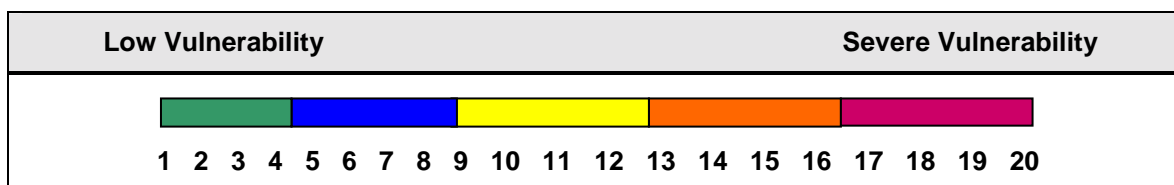
Issues to be considered in selecting your score:

- Do you have an employee occupational health specialist on staff?

- Do you have an occupational health safety program in place?

- Do you have a health professional working at your facility?

- Do you have a procedure in place to track the health of each employee and know if more than one employee has the same symptoms?

- Do you monitor the health status of employees on sick status or absent otherwise?

- Are employees encouraged to keep supervisors informed on any unusual health related event or condition?

- Are employees required to report any unusual conditions or substances encountered in the course of their normal duties, such as strange substances or odors from packaging or mail?

- Do employees know the proper procedures for emergency operation or shut-off of air handler, air circulating or ventilation systems?

- Do you keep a current list of employees, home addresses and emergency contact information?

- Do you have an emergency notification plan for employees (e.g. calling tree)?

18. Capacity to Recognize a Bio-Terrorism Event

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
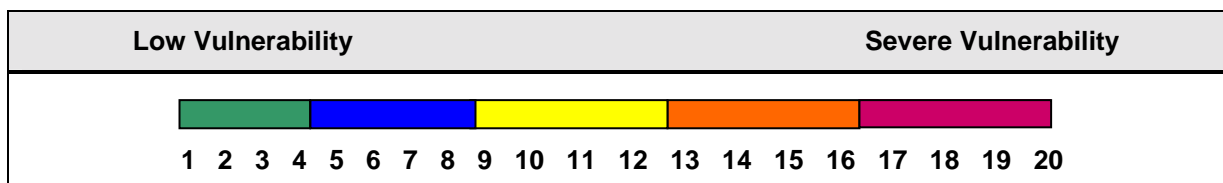
Issues to be considered in selecting your score:

- Do you regularly notify the state or local health department of all reportable diseases and conditions when they occur in your facility?

- Do you have personnel trained in recognizing the clinical signs and symptoms of potential victims of biologic or chemical events?

- Do you have a plan for responding to suspected Bio-Terrorism events?

- Do you regularly exchange information about unusual symptoms or patterns of disease with health care facilities in your area or the local health department?

19. Capacity to Respond to a Bio-Terrorism Event

Low Vulnerability	Severe Vulnerability

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
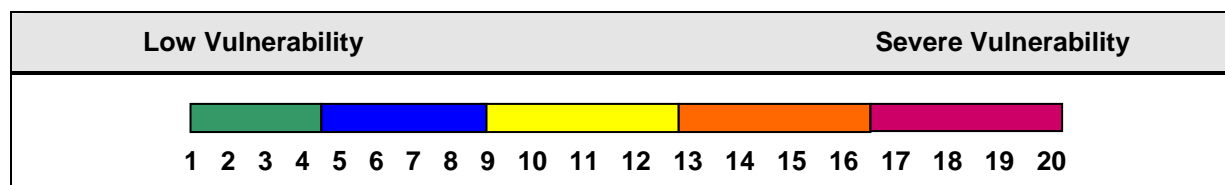
Issues to be considered in selecting your score:

- Do you have a Bio-Terrorism response plan for your facility?

- Have you coordinated your Bio-Terrorism response plan with the local emergency operations team including law enforcement and health care facilities?

- Do you have a system for knowing the bed (or care) capacity of your facility at any given time?

- Do you have a current inventory of your medical supplies and pharmaceuticals that may be required during an emergency event?

- Do you have a plan for contacting and deploying health care personnel during an emergency?

- Do you have plans for how to best utilize your facility during a mass casualty event?

- Do you have decontamination facilities?

- Do you have a protocol for treating contaminated patients?

- Do you have a plan for how to utilize volunteers from other areas and facilities during an emergency? (e.g. Scheduling, Training, Credentialing, etc.)

Self-Assessment Evaluation:

20-72	Low Risk
73-145	Guarded Risk
146-218	Elevated Risk
219-291	High Risk
292-380	Severe Risk

Total Score: _____

It is important to remember that the most important threat reduction measure is vigilance on the part of your organization's staff, their awareness of anything out of the ordinary and their prompt communication of that information to your organization's security team, management or local law enforcement.

Remarks/Unusual or Significant Issues:

Please list any important remarks you think should be made concerning your self-assessment. Also, please list any unusual or significant findings that you developed during your self-assessment, list significant hazardous materials that might be used as a terrorist weapon or any significant impact a terrorist act against your site may cause to the community.

_____

_____

_____

_____

_____

_____

Attach an additional sheet if necessary.

Group Performing Self-Assessment: _____

    Type of Business/Facility: _____

    Contact Person: _____

    Address: _____

        _____

        _____

    Phone No: _____

    Fax No: _____

    E-Mail Address: _____

    (For information sharing ONLY)

Who is Your Local Law Enforcement Contact?

You should coordinate with your local law enforcement agency regarding the results of your self-assessment. If your self-assessment indicates that your score is in the High Risk category, or if you believe your organization presents significant or unusual vulnerability or risk factors, you should provide a copy of this self-assessment to your local law enforcement office.

    Law enforcement office: _____

    Address: _____

        _____

        _____

    Contact name: _____

    Contact phone number: _____

APPENDIX C
TERMS AND ACRONYMS USED IN THIS DOCUMENT

The following terms and acronyms are used within this document

ACCESS refers to A Central Computerized Enforcement Service System which is the primary means of notifying emergency management functions and personnel throughout the state.

AED refers to Automated External Defibrillator and the training provided by the Red Cross.

ARES refers to the Amateur Radio Emergency Service program, contact your local Amateur Radio Club or visit the web site at: http://www.ares.org/

CERT refers to Community Emergency Response Teams, contact the local emergency management agency for details.

COP refers to Community Policing programs, contact your local law enforcement office for programs in your area.

CPR refers to Cardio-Pulmonary Resuscitation and the training provided by the Red Cross.

Critical Infrastructure means the public or private systems, whether physical or virtual, so vital to the United States or the State of Washington that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national or state economic security, national or state public health or safety, or any combination of those matters, including:

Energy - (electrical generation / switching / load dispatch, gas and oil production, nuclear power plants, etc.)

Emergency Services - (emergency operations centers, fire, law enforcement, emergency medical services, etc.)

Information and Telecommunications - (9-1-1 centers, critical tower sites, telephone and communications infrastructure, IT systems, radio and television transmission sites, EAS activation points, etc)

Transportation - (terminals, bridges, ferries, etc.)

Water - (distribution systems and treatment plants, etc.)

Banking and Finance - (including processing facilities, etc.)

Government - (facilities, elected officials, etc.)

Agriculture - (grain storage, animal feed lots, fertilizer storage, etc.)

Food - (food processors, food shippers, etc.)

Public Health - (hospitals, labs, public health districts, etc.)

Defense Industry - (manufacturing, military facilities, etc.)

Chemical Industry - (production, storage, movement, etc.)

Postal and Shipping - (post offices, parcel delivery services, trucking, etc.)

EAS refers to the Emergency Alert System used in coordination with the broadcast industry to provide alert type information essential to the public concerning an emergency.

EMD refers to the Emergency Management Division of the State Military Department.

EOC refers to the state or local Emergency Operations Center for directing activities based on the threat advisory.

EOP refers to Emergency Operations Plan.

HSAS refers to the Homeland Security Advisory System.

HSPD refers to Homeland Security Presidential Directives followed by a dash and number (e.g. HSPD-3).

JIC refers to a Joint Information Center of government public information officials.

Key Assets refer to (office buildings (especially multi-national corporations), religious institutions, public areas, schools, national and local symbols, historical attractions, monuments and icons).

NTWS refers to the Federal Bureau of Investigation National Terrorism Warning System.

PIO refers to a government Public Information Officer.

SEOO refers to the State Emergency Operations Officer who directs emergency operations at the State Emergency Operations Center (EOC).

SOG refers to Standard Operating Guides.

SOP refers to Standard Operating Procedures.

SWAT refers to Special Weapons and Tactics teams.

APPENDIX D

GENERAL PRACTICAL GUIDELINES IN CASE OF AN INCIDENT OR ATTACK

Please note, this information is provided as a basic outline of some practical considerations in case of an incident or attack. This is not intended to be an exhaustive list, but might form the basis for a further list of practical guidelines. There is no perfect list of guidelines. This information was extracted from the Ready.gov website from the U.S. Department of Homeland Security. You can view further information at http://www.ready.gov or by following the various links imbedded below.

Overview

INTRODUCTION - What is Ready.gov all about?

Terrorists are working to obtain biological, chemical, nuclear and radiological weapons and the threat of an attack is very real. Here at the Department of Homeland Security, throughout the federal government, and at organizations across America we are working hard to strengthen our Nation's security. Whenever possible, we want to stop terrorist attacks before they happen. All Americans should begin a process of learning about potential threats so we are better prepared to react during an attack. While there is no way to predict what will happen, or what your personal circumstances will be, there are simple things you can do now to prepare yourself and your loved ones.

Some of the things you can do to prepare for the unexpected, such as assembling a supply kit and developing a family communications plan, are the same for both a natural or man-made emergency. However, as you will see throughout the pages of **Ready.gov**, there are important differences among potential terrorist threats that will impact the decisions you make and the actions you take. With a little planning and common sense, you can be better prepared for the unexpected.

STEP 1 - Make a Kit of Emergency Supplies

Be prepared to improvise and use what you have on hand to make it on your own for *at least* three days, maybe longer. While there are many things that might make you more comfortable, think first about fresh water, food and clean air. Consider putting together two kits. In one, put everything needed to stay where you are and make it on your own. The other should be a lightweight, smaller version you can take with you if you have to get away.

You'll need a gallon of water per person per day. Include in the kits canned and dried foods that are easy to store and prepare. If you live in a cold weather climate, include warm clothes and a sleeping bag for each member of the family.

Start now by gathering basic emergency supplies – a flashlight, a battery-powered radio, extra batteries, a first aid kit, toilet articles, prescription medicines and

other special things your family may need. Many potential terrorist attacks could send tiny microscopic "junk" into the air. Many of these materials can only hurt you if they get into your body, so think about creating a barrier between yourself and any contamination. It's smart to have something for each member of the family that covers their mouth and nose.

Plan to use two to three layers of a cotton t-shirt, handkerchief or towel. Or, consider filter masks, readily available in hardware stores, which are rated based on how small a particle they filter. It is very important that the mask or other material fit your face snugly so that most of the air you breathe comes through the mask, not around it. Do whatever you can to make the best fit possible for children.

Also, include duct tape and heavyweight garbage bags or plastic sheeting that can be used to seal windows and doors if you need to create a barrier between yourself and any potential contamination outside.

STEP 2 - Make a Plan for What You Will Do in an Emergency

Be prepared to assess the situation, use common sense and whatever you have on hand to take care of yourself and your loved ones. Depending on your circumstances and the nature of the attack, the first important decision is deciding whether to stay or go. You should understand and plan for both possibilities.

Develop a Family Communications Plan: Your family may not be together when disaster strikes, so plan how you will contact one another and review what you will do in different situations. Consider a plan where each family member calls, or e-mails, the same friend or relative in the event of an emergency. It may be easier to make a long-distance phone call than to call across town, so an out-of-state contact may be in a better position to communicate among separated family members. You may have trouble getting through, or the phone system may be down altogether, but be patient.

Staying Put: There are circumstances when staying put and creating a barrier between yourself and potentially contaminated air outside, a process known as "shelter-in-place," can be a matter of survival. Choose an interior room or one with as few windows and doors as possible. Consider precutting plastic sheeting to seal windows, doors and air vents. Each piece should be several inches larger than the space you want to cover so that you can duct tape it flat against the wall. Label each piece with the location of where it fits.

If you see large amounts of debris in the air, or if local authorities say the air is badly contaminated, you may want to "shelter-in-place." Quickly bring your family and pets inside, lock doors, and close windows, air vents and fireplace dampers. Immediately turn off air conditioning, forced air heating systems, exhaust fans and clothes dryers. Take your emergency supplies and go into the room you have designated. Seal all windows, doors and vents. Watch TV, listen to the radio or

check the Internet for instructions.

Getting Away: Plan in advance how you will assemble your family and anticipate where you will go. Choose several destinations in different directions so you have options in an emergency. If you have a car, keep at least a half tank of gas in it at all times. Become familiar with alternate routes as well as other means of transportation out of your area. If you do not have a car, plan how you will leave if you have to. Take your emergency supply kit and lock the door behind you. If you believe the air may be contaminated, drive with your windows and vents closed and keep the air conditioning and heater turned off. Listen to the radio for instructions.

At Work and School: Think about the places where your family spends time: school, work and other places you frequent. Talk to your children's schools and your employer about emergency plans. Find out how they will communicate with families during an emergency. If you are an employer, be sure you have an emergency preparedness plan. Review and practice it with your employees. A community working together during an emergency also makes sense. Talk to your neighbors about how you can work together.

STEP 3 - Be Informed about what might happen

Some of the things you can do to prepare for the unexpected, such as assembling a supply kit and developing a family communications plan, are the same for both a natural or man-made emergency. However there are important differences among potential terrorist threats that will impact the decisions you make and the actions you take.

Specific Terrorist Threats

A biological attack is the deliberate release of germs or other substances that can make you sick. Many agents must be inhaled, enter through a cut in the skin or eaten to make you sick.

A chemical attack is the deliberate release of a toxic gas, liquid or solid that can poison people and the environment.

A nuclear blast is an explosion with intense light and heat, a damaging pressure wave and widespread radioactive material that can contaminate the air, water and ground surfaces for miles around.

A radiation threat or "Dirty Bomb" is the use of common explosives to spread radioactive materials over a targeted area.

Be prepared to adapt this information to your personal circumstances and make every effort to follow instructions received from authorities on the scene. Above all, stay calm, be patient and think before you act. With these simple preparations, you can be ready for the unexpected.

APPENDIX E

County Emergency Management Agencies in Washington State

County	Agency Name/URL	Address	Phone/Fax	Director/Contact Email
Adams	Adams County DEM http://www.co.adams.wa.us	2069 W Highway 26 Othello WA 99344	509-488-2061 Fax: 509-659-1724	jayw@co.adams.wa.us
Asotin	Asotin County DEM	PO Box 250 Asotin WA 99402-0250	509-243-2088 Fax: 509-243-2087	Butch Aiken butchacdem@clarkston.com
Benton	Benton County Emergency Services	651 Truman Avenue Richland WA 99352-9104	509-628-2600 Fax: 509-628-2621	Lorlee Mizell l.mizell@bces.wa.gov
Chelan	Chelan County Sheriff's Office http://www.chelancounty.wa.us	401 Washington St Wenatchee WA 98801-0036	(509) 667-6863 Fax: 509-667-6510	John Fleckenstein john.fleckenstein@co.chelan.wa.us
Clallam	Clallam County Emergency Management Division	223 E. 4th St, Ste 6 Port Angeles WA 98362-0149	360-417-2305 Fax: 360-417-2485	Joe Cairlo jcairlo@co.clallam.wa.us
Clark	Clark Regional Emergency Services Agency (CRESA) http://www.clark.wa.us/emergency	710 West 13th St. Vancouver WA 98660-2810	360-737-1911 Fax: 360-694-1954	John Talbot john.talbot@co.clark.wa.us
Columbia	Columbia County DEM http://www.columbiaco.com	535 Cameron St PO Box 5 Dayton WA 99328	509-382-2534 Fax: 509-382-4724	Roger Trump rgtcolco@bmi.net
Cowlitz	Cowlitz County DEM http://www.co.cowlitz.wa.us/dem/	Hall of Justice 312 SW 1st Ave Kelso WA 98626	360-577-3130 Fax: 360-577-3009	Trudy Winterfeld cceoc@kalama.com
Douglas	Douglas County DEM http://www.douglascountysheriff.org	Administrative Building 110 NE 3rd St East Wenatchee WA 98802-4846	509-884-0941 Fax: 509-886-1045	Dan LaRoche dlaroche@co.douglas.wa.us
Ferry	Ferry County DEM	PO Box 1099 Republic WA 99166-1099	1800-342-4344 Fax: 509-775-2127 (Jail)	Pete Werner fcso@rcabletv.com
Franklin	Franklin County EM http://www.franklinem.org	502 Boeing St Pasco WA 99301	509-545-3546 Fax: 509-545-2139	John Scheer jscheer@co.franklin.wa.us
Garfield	Garfield County DEM	PO Box 885 Pomeroy WA 99347	509-843-3369 Fax: 509-843-3567 hm	Clay Barr barrsl@pomeroy-wa.com
Grant	Grant County DEM	6500 32nd Ave NE Suite 911 Moses Lake WA 98837	509-762-1462/64 Fax: 509-762-1465	Sam Lorenz gcem@grantcounty-wa.com
Grays Harbor	Grays Harbor Emergency and Risk Management http://www.grays-harbor.wa.us	310 W. Spruce Suite 212 PO Box 790 Montesano WA 98563	360-249-3911 Fax: 360-249-3805	Mary Davis mdavis@co.grays-harbor.wa.us
Island	Island County Department of Emergency Services	PO Box 5000 Coupeville WA 98239	360-679-7370 Fax: 360-679-7376	T.J. Harmon tjharmon@co.island.wa.us
Jefferson	Jefferson County DEM http://www.co.jefferson.wa.us	81 Elkins Road Port Hadlock WA 98339	360-385-3831 ext. 528/529 Fax: 360-379-0513	Charles Saddler jcdem@co.jefferson.wa.us
King	King County Office of EM http://www.metrokc.gov	7300 Perimeter Rd Rm 128 Seattle WA 98108-3848	206-296-3830 Fax: 206-296-3838	Eric Holdeman eric.holdeman@metrokc.gov
King County Sheriff	King County Sheriff's Special Operations http://www.metrokc.gov/sheriff/	7300 Perimeter Rd S Rm 143 Seattle WA 98108-3849	206-296-3853 Fax: 206-205-8282 (SAR24 hr.)	Ron Ryals ron.ryals@metrokc.gov

County	Agency	Address	Phone	Contact
Kitsap	Kitsap County DEM http://www.kitsapdem.org	1720 Warren Ave Bremerton WA 98337	360-616-5870 Fax: 360-478-9802	Phyllis Mann dem@co.kitsap.wa.us
Kittitas	Kittitas County Sheriff's Office http://www.co.kittitas.wa.us	205 W 5th Ave Ellensburg WA 98926	509-962-7525 Fax: 509-962-7599	Gene Dana danag@co.kittitas.wa.us
Klickitat	Klickitat County Division of Emergency Management	205 S Columbus Ave MS Ch-7 Goldendale WA 98620	509-773-2376 Fax: 509-773-6387	schapple@co.klickitat.wa.us
Lewis	Lewis County Division of Emergency Management http://www.co.lewis.wa.us/ sheriff/dem.htm	350 N Market Blvd Chehalis WA 98532- 1900	360-740-1151 Fax: 360-740-1471	Steve Mansfield sbmansfi@co.lewis.wa.us
Lincoln	Lincoln County Department of Emergency Services http://www.lcso.cc	404 Sinclair PO Box 367 Davenport WA 99122	509-725-9263 Fax: 509-725-3533	Wade Magers wmagers@co.lincoln.wa.us
Mason	Mason County DEM http://www.des.co.mason.wa.us	410 W Business Park Rd Shelton WA 98584- 2870	360-427-7535 Fax: 360-427-7756	Sandi Loertscher mcdes@des.co.mason.wa.us
Okanogan	Okanogan County Sheriff's Office http://www.okanogancounty.org/sheriff/	149 4th Ave. N. PO Box 1490 Okanogan WA 98812	509-422-7206/7204 Fax: 509-422-7236	frogers@co.okanogan.wa.us
Pacific	Pacific County Emergency Management Agency http://www.co.pacific.wa.us/pcema	300 Memorial Dr PO Box 101 South Bend WA 98586-0101	360-875-9340 Fax: 360-875-9342	Stephanie Fritts sfritts@co.pacific.wa.us
Pend Oreille	Pend Oreille County DEM	PO Box 5035 Newport WA 99156- 5035	509-447-3731 Fax: 509-447-0286	JoAnn Boggs jboggs@povn.com
Pierce	Pierce County DEM http://www.co.pierce.wa.us/dem	901 Tacoma Ave S, Ste 300 Tacoma WA 98402- 2102	253-798-6595 (DEM) Fax: 253-798-6624 (EOC)	Steve Bailey sbailey@co.pierce.wa.us
San Juan	San Juan County Sheriff's Office http://www.co.san-juan.wa.us/ sheriff/index.asp	PO Box 669 Friday Harbor WA 98250	360-378-4151 Fax: 360-378-7125	carlp@co.san-juan.wa.us
Skagit	Skagit County DEM http://www.skagitcounty.net	2911 E College Way Suite B Mount Vernon WA 98273	360-428-3250 Fax: 360-428-3255	Tom Sheahan dem@co.skagit.wa.us
Skamania	Skamania County DEM http://www.emy-management.org	PO Box 790 Stevenson WA 98648	509-427-8076 Fax: 509-427-7555	Karl Tesch ktesch@co.skamania.wa.us
Snohomish	Snohomish County DEM http://www.snodem.org	3509 109th St SW Everett WA 98204	425-423-7635 Fax: 425-423-9152	Roger Serra rserra@snodem.org
Spokane	Spokane County DEM http://www.spokanecounty.org	W 1121 Gardner Spokane WA 99201- 2072	509-477-2204 Fax: 509-477-5759	Dave Byrnes dbyrnes@spokancounty.org
Stevens	Stevens County Department of Emergency Services	PO Box 186 Colville WA 99114	509-684-5296 Fax: 509-684-7583	Tina Cannon tcannon@co.stevens.wa.us
Thurston	Thurston County Emergency Management http://www.co.thurston.wa.us/em	2703 Pacific Ave SE Suite B Olympia WA 98501- 2036	360-754-3360 Fax: 360-704-2775	Bette Shultz emwebmaster@co.thurston.wa.us
Wahkiakum	Wahkiakum County DEM http://www.sd.co.wahkiakum.wa.us	64 Maine St PO Box 65 Cathlamet WA 98612	360-795-3242 Fax: 360-795-3145	Dolly Tawater dollyt@sd.co.wahkiakum.wa.us
Walla Walla	Walla Walla County Emergency Management Division	27 N 2nd Ave Walla Walla WA 99362	509-527-3223 Fax: 509-527-3263	Dan Marlatt emd@co.walla-walla.wa.us

Whatcom	Whatcom County DEM http://www.co.whatcom.wa.us/dem	311 Grand Ave Suite B-08 Bellingham WA 98225	360-676-6681 Fax: 360-738-2518	Neil Clement wcdem@co.whatcom.wa.us
Whitman	Whitman County DEM	310 Main Colfax WA 99111	509-332-2521 Fax: 509-397-2099	Steve Tomson emergserv@co.whitman.wa.us
Yakima	Yakima Valley Office of Emergency Management http://www.pan.co.yakima.wa.us	128 N 2nd St Rm B-10 Yakima WA 98901	509-574-1900 Fax: 509-574-1901	Jim Hall jim.hall@co.yakima.wa.us

Contact:

Please contact Al Josue, a.josue@emd.wa.gov, 253-512-7037, Fax: 253-512-7203 if you have any questions regarding this document.

WASHINGTON MILITARY DEPARTMENT
STATE EMERGENCY MANAGEMENT DIVISION
CONTACT INFORMATION

Main Administrative Numbers: 253-512-7000 or 800-562-6108	
EMD Mailing Address:	Washington Military Department Emergency Management Division Building 20, M/S: TA-20 Camp Murray, WA 98430-5122

APPENDIX F

Municipal Emergency Management Agencies in Washington State

City	Agency Name/URL	Address	Phone/Fax	Director/Contact Email
Auburn	Auburn Department of Emergency Services http://http://www.ci.auburn.wa.us	1101 D St NE Auburn WA 98002-4016	253-931-3060 Fax: 253-931-3055	Bob Johnson bjohnso@ci.auburn.wa.us
Bellevue	Bellevue Fire Department Emergency Preparedness Division http://www.ci.bellevue.wa.us	11501 Main St PO Box 90012 Bellevue WA 98009-9012	425-452-7923 Fax: 425-452-2840	Barb Graff bgraff@ci.bellevue.wa.us
Buckley	DEM Police Department http://www.cityofbuckley.com/	PO Box 640 Buckley WA 98321	253-862-9059 Fax: 360-829-0133	bfd@tx3.net
Cheney	Department of Emergency Services Fire Department http://www.ci.cheney.wa.us/	611 Fourth St Cheney WA 99004	509-235-7291 Fax: 509-235-7244	John Montague cheneyfd@ci.cheney.wa.us
Ellensburg	Fire Department http://www.ci.ellensburg.wa.us	102 N Pearl St Ellensburg WA 98926	509-962-7299 Fax: 509-962-7254	rschmidt@firemednet.org
ESCA	Emergency Services Coordinating Agency (ESCA) http://esca1.home.mindspring.com/esca/	23607 Hwy 99 Suite 3-C Edmonds WA 98026-9272	425-776-3722 (Emer) Fax: 425-775-7153	Lynn Gross esca1@mindspring.com
Federal Way	DEM c/o Federal Way City Hall http://www.ci.federal-way.wa.us	PO Box 9718 Federal Way WA 98063-9718	253-661-4131 Fax: 253-661-4129	Cary Roe cary.roe@ci.federal-way.wa.us
Issaquah	DEM City of Issaquah http://www.ci.issaquah.wa.us	PO Box 1307 Issaquah WA 98027	425-837-3470 Fax: 425-837-3479	Bret Heath breth@ci.issaquah.wa.us
Kent	Emergency Management http://www.ci.kent.wa.us/fireprevention/emergencymanagement/default.htm	24611 116th Ave. SE Kent WA 98030-4939	253-856-4340 Fax: 253-856-4119	Albert Bond KENTECC@ci.kent.wa.us
Kirkland	DEM Emergency Preparedness Services http://www.ci.kirkland.wa.us	123 5th Ave Kirkland WA 98033	425-828-1143 Fax: 425-828-1292	jhenderson@ci.kirkland.wa.us
Lacey	City of Lacey http://www.wa.gov/lacey	420 College St. S.E. PO Box 3400 Lacey WA 98509-3400	360-438-2654 Fax: 360-456-7798	Ed Sorger esorger@ci.lacey.wa.us
Mercer Island	City of Mercer Island http://www.ci.mercer-island.wa.us	9611 SE 36th St Mercer Island WA 98040	206-236-3576 Fax: 206-236-3659	Dee Totten dee.totten@ci.mercer-island.wa.us
Normandy Park	DEM City of Normandy Park http://www.ci.normandy-park.wa.us/	801 SW 174th St Normandy Park WA 98166	206-248-7600 Fax: 206-246-9732	police@ci.normandy-park.wa.us
Olympia	DEM Olympia Fire Department http://www.ci.olympia.wa.us	100 Eastside St NE Olympia WA 98506	360-753-8348 Fax: 360-753-8054	Greg Wright gwright@ci.olympia.wa.us
Port Angeles	DEM Port Angeles FD http://www.ci.port-angeles.wa.us	102 E 5th St Port Angeles WA 98362-3014	360-417-4655 Fax: 360-417-4659	Dan McKeen dmckeen@ci.port-angeles.wa.gov
Pullman	City of Pullman, DES http://www.ci.pullman.wa.us/police	260 SE Kamiaken PO Box 249 Pullman WA 99163	509-334-0802 Fax: 509-332-0829	Ted Weatherly ted.weatherly@ci.pullman.wa.us
Puyallup	DEM http://www.puyallupfire.com	902 Seventh St. NW Puyallup WA 98371	253-845-6666 Fax: 253-770-3333	Merle Frank merle@ci.puyallup.wa.us
Redmond	DEM http://www.ci.redmond.wa.us	8450 161st Ave NE Redmond WA 98052-3584	425-556-2200 Fax: 425-556-2227	Robert Schneider rschneider@ci.redmond.wa.us

Renton	DEM Renton Fire Department http://www.ci.renton.wa.us	1055 S Grady Way Renton WA 98055	425-430-7000 Fax: 425-430-7044	ggordon@ci.renton.wa.us
Seattle	DEM, City of Seattle http://www.cityofseattle.net/ Emergencygency_mgt/	2320 Fourth Ave Seattle WA 98121-1718	206-233-5076 Fax: 206-684-5998	Jim Mullen Jim.mullen@seattle.wa.us
Shelton	City of Shelton http://www.geocities.com/ pipeline/dropzone/4236	PO Box 1277 Shelton WA 98584	360-426-3348 Fax: 360-427-9438	jghig@ci.shelton.wa.us
Skykomish	DEM	West 107 Cascade Hwy PO Box 311 Skykomish WA 98288	360-677-2686 Fax: 360-677-2574	volfire50@starband.net
Snoqualmie	Department of Public Safety http://www.ci.snoqualmie.wa.us	34825 SE Douglas St Snoqualmie WA 98065	425-888-2332 Fax: 425-831-6121	chief@ci.snoqualmie.wa.us
Tacoma	Tacoma Emergency Services http://www.ci.tacoma.wa.us/default.asp	901 S. Faucett St. Tacoma WA 98402	253-591-5798 Fax: 253-591-5746	Jeff Jenson jjensen@ci.tacoma.wa.us
Tukwila	DES http://www.ci.tukwila.wa.us	6300 Southcenter Blvd Suite 100 Tukwila WA 98188-2544	206-433-0179 Fax: 206-431-3665	jmorrow@ci.tukwila.wa.us
Tumwater	Tumwater DES http://www.tumwater.wa.us	555 Israel Road SW (Mailing Address) Tumwater WA 98501	360-754-4170 Fax: 360-754-4179	bburton@ci.tumwater.wa.us
Woodinville	Emergency Management Director http://www.woodenville-city.com	17301 133 Ave. NE Woodinville WA 98072-8563	425-877-2281 Fax: 425-489-2705	Ray Sturtz rays@ci.woodinville.wa.us
Yelm	City of Yelm Police Department	118 Mosman Ave SE PO Box 479 Yelm WA 98597	360-458-5701 Fax: 360-458-3188	yelmpd@ywave.com

Contact:

Please contact Al Josue, a.josue@emd.wa.gov, 253-512-7037, Fax: 253-512-7203 if you have any questions regarding this document.

WASHINGTON MILITARY DEPARTMENT
STATE EMERGENCY MANAGEMENT DIVISION
CONTACT INFORMATION

Main Administrative Numbers: 253-512-7000 or 800-562-6108	
EMD Mailing Address:	Washington Military Department Emergency Management Division Building 20, M/S: TA-20 Camp Murray, WA 98430-5122

APPENDIX G

LOCAL RED CROSS CHAPTERS

ANACORTES/SAN JUAN ISLAND

2900 T Avenue Suite A
Anacortes, WA 98221
Phone: (360) 293-2911
Fax: (360) 293-0101

BELLINGHAM

2111 King Street
Bellingham, WA 98225
Phone: (360) 733-3290
Fax: (360) 738-4014

BREMERTON

PO Box 499
811 Pacific Ave.
Bremerton, WA 98337
Phone: (360) 377-3761
Fax: (360) 792-0498

EVERETT

2530 Lombard Avenue
Everett, Washington 98201
Phone: (425) 252-4103

LONGVIEW

1265 14th Ave
Longview, WA 98632
Phone: (360) 423-7880
Fax: (360) 423-7882

MOUNT VERNON

119 S 14th St
Mount Vernon, WA 98274
Phone: (360) 424-5291
Fax: (360) 424-8623

OAK HARBOR

1010 West Ault Field Rd
Oak Harbor, WA 98278
Phone: (360) 257-2096
or (360)257-2879

OLYMPIA

2618 Twelfth Ct SW
Olympia, WA 98507
Phone: (360) 352-8575
Fax: (360) 352-0861

PULLMAN

115 NW State Street
Suite 313, Box 29
Pullman, WA 99163
Phone: (509) 332-2304
1- 877-397-2901
Fax: (509) 332-3725

SEATTLE

1900 25th Avenue South
Seattle, WA 98144-4708
Phone: (206) 323-2345
Fax: (206) 325-8211

SPOKANE

315 West Nora Avenue
Spokane, WA 99205
Phone: (509) 326-3330
Fax (509) 326-3336

TACOMA

1235 South Tacoma Way
Tacoma, WA 98409
Phone: (253) 474-0400
Fax: (253) 473-4843

TRI-CITIES

7202 West Deschutes
Kennewick, WA 99336
Phone: (509) 783-6195
Fax: (509) 736-0586

VANCOUVER

3114 E 4th Plain
Vancouver, WA 98661
Phone: (360) 693-5821
Fax: (360) 693-1953

WENATCHEE

12 Orondo Ave
Wenatchee, WA 98801
Phone: (509) 663-3907
1-800-218-0493
Fax: (509) 663-9061

WALLA WALLA

175 S. Park
Walla Walla, WA 99362
Phone: (509) 525.7380
Fax: (509) 527.1269

YAKIMA

302 South 2nd Street
Yakima, WA 98901
Phone: (509) 457-1690
Fax: (509) 576-0898

APPENDIX H

INTERNET ADDRESS LINKS TO REFERENCED INFORMATION

On-line version of this guide
http://emd.wa.gov/site-general/wahsas/wa-hsas-idx.htm

Homeland Security Presidential Decision (HSPD)-3
http://www.fas.org/irp/offdocs/nspd/hspd-3.htm

National Department of Homeland Security Web Site
http://www.dhs.gov/dhspublic/

Terrorism: Preparing for the Unexpected
http://www.redcross.org/services/disaster/keepsafe/terrorism.pdf

Preparing Your Business for the Unthinkable
http://www.redcross.org/services/disaster/beprepared/unthinkable2.pdf

Emergency Management Guide for Business and Industry
http://www.redcross.org/services/disaster/beprepared/busi_industry.html#fema

"Masters of Disaster" K-12 Education Curriculum
http://www.redcross.org/disaster/masters/

"Masters of Disaster" K-12 Education Curriculum- "Facing Fear: Helping Young People Deal with Terrorism and Tragic Events"
http://www.redcross.org/disaster/masters/facingfear/

Your Family Disaster Plan
http://www.redcross.org/services/disaster/beprepared/fdpall.pdf

Your Family Disaster Supplies Kit
http://www.redcross.org/disaster/safety/fdsk.pdf

Citizen Corps
http://www.citizencorps.gov/

Citizen Preparedness Guide
http://www.weprevent.org/usa/cover.pdf

Amateur Radio Emergency Services System
http://www.ares.org/

Community Emergency Response Team ("CERT") Materials
http://training.fema.gov/EMIWeb/CERT/mtrls.asp

Are You Ready? A Guide to Citizen Preparedness
http://www.fema.gov/areyouready/

Be Ready Campaign from the Department of Homeland Security
http://www.ready.gov/

Washington Military Department Emergency Management Division
http://emd.wa.gov/